INF-019G

E-Commerce Guideline

Purpose

This e-commerce guideline is also to be used as an overview in the management of Coast Mountain College's (CMTN's) electronic services.

Overview

CMTN recognizes the importance of electronic commerce (e commerce) activities to its present-day operations.

CMTN is committed to using e-commerce activities in a cost-effective manner that promotes accuracy, safety, security, and efficiency. These activities bring automation and efficiencies to traditional manual tasks and allow quick access to information resulting in improved member service.

Definitions

Authentication: The process of determining whether someone or something is, in fact, who or what it is declared to be. Depending on the transactions, a more stringent authentication process may be required.

Automated Teller Machine (ATM): A self-service banking outlet that allows users to withdraw money, check their balance, or transfer funds.

Electronic Commerce: Electronic financial services delivered via electronic means including, but not limited to, the Internet or other electronic delivery vehicles. Examples of e-commerce activities include:

- Internet/world wide web services:
  - email inquiries and responses
  - publishing of general information on CMTN website
  - data entry or verification by staff on a vendor's data processing system
  - file transfers of member information for direct mail projects or statement generation
- web account access:
  - viewing share or loan transaction history and balances
  - transferring funds between shares and loans, transfers to other financials, or person-to-person transfers (PTPs)
  - requesting a cheque withdrawal from a share or loan

  - applying for CMTN services through applications or forms
  - email statements
  - electronic retrieval of cheque copies
  - e-alerts
- online bill-paying services
- audio response/phone-based
- wireless services
- mobile banking.

Encryption: The conversion of data into a form, called a cipher text, which cannot be easily understood by unauthorized people.

Firewall: Any hardware and/or software designed to examine network traffic using policy statements (ruleset) to block unauthorized access while permitting authorized communications to or from a network or electronic equipment.

Scope

This guideline applies to all CMTN E-commerce activities, including CMTN's website, email, telephone access system, ACH transactions, ATM system, online bill payment, and home banking services. E-commerce activities also include business-to-business transactions where interaction is conducted electronically between CMTN and its business partners using the Internet as the communications network.

Details

CMTN's Commitment

CMTN is committed to enhancing member service through the use of many forms of e commerce activities.

CMTN safeguards member data at all times, including the processing of e-commerce transactions.

- Information must be protected at both the sending and receiving ends of each transaction. To accomplish this, several levels of protection are applied to e commerce activities.

Encryption

Encrypting transactions provides security by ensuring that no portion of a transaction is readable except by the parties at each end of the transmission.

Encryption:

- ensures that data can be transmitted securely without concern that another party could intercept all or part of the transaction
- makes certain that the transaction is not tampered with as it routes from point to point and data is received exactly as it was sent.

CMTN will use a minimum of 128b encryption. This also applies to vendors that host CMTN member data.

Authentication

After a secure connection is established, the initiating party must prove his/her identity before conducting the transaction.

- This is typically handled with user IDs or account numbers, along with password or PIN combinations.
- Encryption certificates are also used to validate the authenticity of both servers and users.

System administrators control system access by assigning users different levels of access for applications and data.

- These access levels are determined by senior management and are specific to each job function.
- This ensures that access to applications and specific types of transactions are only granted as job functions require.

Multi-Factor Authentication (MFA)

For online banking, MFA offers more than one form of authentication to verify the legitimacy of a transaction.

The layered defense makes it more difficult for an unauthorized person to gain access.

Firewalls

CMTN will deploy and utilize firewalls as necessary to protect internal systems from threats originating from the Internet, as well as those that might be present when connecting to vendors' networks.

Firewall operating systems and configurations will be reviewed periodically to ensure maximum protection.

An audit log will be maintained tracking all attempts to access un-configured (blocked) services.

Firewalls and other access devices will be used, as needed, to limit access to sites or services that are deemed inappropriate or of a non-corporate nature.

Vendor-hosted solution firewalls will be reviewed before implementation.

Network Traffic Rules and Restrictions

Intra-network traffic is subject to distinct operating rules and restrictions.

- Through the use of firewall technology, outside parties are directed only to approved, internal resources.
- An example of this is web page services that allow certain types of traffic from the Internet (web page browsing) but have other types of traffic blocked (e.g., administrative tasks). This strategy dramatically reduces the risk of any party gaining unauthorized access to a protected server.

The internal network is also protected from virus attacks through the use of network-level anti-virus software that is updated automatically on a regular basis.

- These regular updates:
  - are loaded automatically to each PC, as they become available
  - provide the most up-to-date virus protection and security available.
- Email is also scanned before delivery, reducing the potential of a virus entering the network in this manner.

Physical Site Security

The entire IT Department is protected by a card access entry system allowing only authorized personnel into the department.

Sensitive data, hardware, and software are secured in the CMTN data centre, which is secured with a card access entry point and is monitored throughout the day by IT staff.

- Access to the data centre is further limited to a small number of authorized personnel.
- CMTN changes administrative passwords and immediately removes card access privileges after any change in IT staff.

CMTN stores overnight backups of critical systems data and replicated storage area network (SAN) storage to a secure, off-site location to ensure that data is available in the event of a disaster or other critical situation.

Staff Training and Review

IT staff receives training and reviews all procedures at least annually or as major system additions or changes are implemented.

User Password Maintenance

Staff passwords, on the host data processing system, expire after 45 or 90 days, forcing users to modify their passwords.

This control, along with INF-008G, *Password Choice and Protection Guideline,* which prohibits users from sharing or disclosing their passwords, is intended to prohibit unauthorized access to systems and data.

After receiving a change in status from the Human Resources Department or other management team members, IT staff immediately removes user access codes from appropriate systems.

Expert Assistance

CMTN recognizes that e-commerce security issues change daily. New threats to security, safety, and accuracy appear daily and system vendors publish updates and patches regularly to eliminate the threat.

To assist in the ongoing maintenance of key components of system security, CMTN will engage, at regularly scheduled intervals, consulting and audit oversight with a nationally recognized leader in the area of e-commerce security.

This vendor may also provide technical assistance as new e-commerce related features are added to the system to ensure the continued safety and security of existing systems.

Communications Network

CMTN employs the use of several types of data communication lines including dial-up phone lines, direct point-to-point circuits, and other private and public network connections.

Data transmissions are secured, encrypted, and/or password protected, as needed.

Response Program

In the event that CMTN suspects or detects unauthorized individuals have gained access to member information systems, CMTN will report such actions to appropriate regulatory and law enforcement agencies according to CMTN’s INF-002, Security Incident Management Policy.

Related Policies, Guidelines and Other Resources

- INF-008G, *Password Choice and Protection Guideline*